新しいアダマール行列の構成法(代数的組合せ論)

AUTHOR(S):

宮本, 雅彦

CITATION:

宮本, 雅彦. 新しいアダマール行列の構成法(代数的組合せ論). 数理解析研究所講究録 1988, 671: 55-65

ISSUE DATE:

1988-09

URL:

http://hdl.handle.net/2433/100824

数理解析研究所講究録
671巻 1988年 55-65

新しいアダマール行列の構成法

愛媛大学　理　宮本雅彦

アダマール行列とは、成分が1又は－1だけから成る正方行列Hで各行が互に直交しているものをいう。（この様に各行がお互に直交している正方行列をこれから直交行列と呼ぶ。）　特に、Hがn×n正方行列の時、このnをアダマール行列の次数と呼ぶ。この時 $HH^t = nI_n$ となる。ここで、H^t はHの転置行列、I_n はn次の単位行列を表す。このアダマール行列は組合せ理論の色々な分野と関係しており興味ある性質をもっているが、此では、アダマール行列の存在についてのみ話を進めたい。アダマール行列が存在すれば、その次数は1か2か又は4の倍数となる事が分るが、この逆が成立つだろうというのが、アダマール行列に関しての最大の問題であり、アダマール予想と呼ばれている。もしn次のアダマール行列が存在すれば2n次のアダマール行列も存在するので奇数のnに対して4n次のアダマール行列の存在を示せば充分である。今まで色々な系列の次数に対してアダマール行列が構成されているが、それらは非常に粗く等差数列的な次数に対するアダマール行列の構成

は見つかっていない。　又、拡大という事に関しても、４ｓ次のアダマール行列と４ｔ次のアダマール行列とから、４ｓｔ次のアダマール行列を構成する方法は現在のところ、４ｓ次のBauert-Hall型と４ｔ次のWilliamson型から４ｓｔ次のアダマール行列を構成する方法しかなく、それ以上の拡大を構成できない。

ここでは、かなり多くの新しい次数を持つアダマール行列を紹介します。　此で紹介する構成法によって次数４ｎ（ｎは奇数）で８０００以下のものを調べると　A.V.GermitaとJ.Seberryの本　”Orthogonal Designs”の中の表と最近の結果によれば、２１５個の次数に対してアダマール行列の存在が判っていなかったが、此では、このうち８９個の次数に対してアダマール行列を構成した。これにより残りは１２６個となる。さらに、残りの次数に対しても４ｎ次での存在は示せないが、多くの次数に対しては、８ｎ次のアダマール行列を構成した。　これらの結果は最後に表にして載せた。

定理１．　ｑを奇素数巾とし、ｑ≡１（法４）とする。もし　ｑ－１次のアダマール行列が存在すれば、４ｑ次のアダマール行列も存在する。

この定理の証明は複素アダマール行列や四元数アダマール行列に対しても有効なので次の結果を得た。

系２．　　ｑを奇素数巾とする。　もし２(q+1)次の複素型のアダマール行列が存在すれば、８ｑ次のアダマール行列も存在する。　又、もし、４(q-1)次のWilliamson型のアダマール行列が存在すれば、１６ｑ次のアダマール行列も存在する。

系３．　　ｑを奇素数巾とし、　ｑ≡３（法４）とする。　もし２ｑ-３又はｑ-２が素数巾なら、８ｑ次のアダマール行列が存在する。

ここで、複素型のアダマール行列とは、

$$H = \begin{bmatrix} A & B \\ -B & A \end{bmatrix}$$

の形を持つアダマール行列の事をいう。　この時、

$AB^t = BA^t$　が成立つが、この性質を”ＡとＢがアミカブル”と呼ぶ事にする。　もし　Ａ，Ｂともに対称行列の時には、Ｈを対称複素型と呼ぶ。　２ｔ次の複素型のアダマール行列が存在する事と　ｔ次の複素アダマール行列が存在する

こととは同値である。

次にこれから構成するアダマール行列は、一番最初に話したように拡大の時に重要な役割を果たすWilliamson型のアダマール行列である。

定理４．　q を奇素数巾とし、q ≡ 1（法４）とする。もし対称複素型の q－1 次のアダマール行列が存在すれば、４q 次のWilliamson型のアダマール行列が存在する。

系５．　q を奇素数巾とし、q ≡ 1（法４）とする。もし $\frac{1}{2}$（q－3）が素数巾であるか又は、複素型の q－1 次のアダマール行列が存在すれば、４q 次のWilliamson型のアダマール行列が存在する。

定理６．　q を奇素数巾とし、q ≡ 1（法４）とする。もし対称複素型の q＋1 次のＣ－行列と対称複素型の q＋3 次の C_2- 行列が存在すれば、４（q＋２）次のWilliamson型のアダマール行列が存在する。

ここで、Ｃ-行列とは、対角成分がすべて０であり、

その他の成分が 1 又は -1 であるような直交行列の事をいう。又、C_2- 行列とは、2t×2t正方行列 $D=(d_{i,j})$ で対角成分で $d_{i,i+t}$ と $d_{i+t,i}$ とが $i=1,\ldots,t$ に対して0であり、その他の成分はすべて 1 又は -1 となっている直交行列のことをいう。

これらの結果によって 8000までの次数に対して調べると以下の新しい次数4nに対してアダマール行列の存在を証明した。 n =

219, 249, 267, 269, 303, 373, 445, 509, 515, 519, 581,
613, 623, 657, 699, 721, 723, 733, 757, 763, 773, 803,
857, 865, 913, 941, 949, 959, 965, 979, 985, 1043, 1047,
1059, 1079, 1109, 1133, 1157, 1165, 1199, 1205, 1211, 1213, 1227,
1241, 1243, 1299, 1301, 1335, 1341, 1351, 1359, 1373, 1379, 1381,
1385, 1387, 1397, 1411, 1433, 1465, 1469, 1493, 1507, 1513, 1527,
1557, 1577, 1631, 1639, 1661, 1671, 1679, 1693, 1745, 1751, 1753,
1781, 1869, 1903, 1909, 1913, 1921, 1937, 1957, 1963, 1973, 1985,
1993

§2. この節で前節で述べた各結果の証明を与える。前節の結果はすべてこの節で示す主定理の系として出てくる。 此では、アダマール行列の構成を考えるが、その前に、少しこれから使う記号の説明をしよう。

記号 $e=e_m$ で全成分が1である様な1×m行

列を表す。　m×m行列　M　に対して、e(M)=s　は　$Me_m^t = se_m$　と　$e_m M = se_m$　の両方を意味する。　$J=J_m$　で全成分が1であるようなm×m行列を表す。4個のk×h行列　A、B、C、D　と16個のk×h行列　X_{ij}　(i,j=1,..,4)に対して、W(A,B,C,D)と　W(X_{ij})とによって、

$$W(A,B,C,D) = \begin{bmatrix} A & B & C & D \\ -B & A & D & -C \\ -C & -D & A & B \\ -D & C & -B & A \end{bmatrix}$$

と

$$W(X_{ij}) = \begin{bmatrix} X_{11} & X_{12} & X_{13} & X_{14} \\ -X_{21} & X_{22} & X_{23} & -X_{24} \\ -X_{31} & -X_{32} & X_{33} & X_{34} \\ -X_{41} & X_{42} & -X_{43} & X_{44} \end{bmatrix}$$

とをそれぞれ表すことにする。

特に、A，B，C，D　がおたがいにアミカブルである様なときには、W(A,B,C,D)を”Williamson型”と呼ぶことにする。さらに　X_{1i}　(i=1,...,4)がお互にアミカブルで　$W(X_{ij}) = W(X_{11}, X_{12}, X_{13}, X_{14})$の時に、$W(X_{ij})$　を”Williamson型”と呼ぶ。

さて、これから4(2m+1)次のアダマール行列の構成を目指す。まず2組の16個づつからなるm×m行列　U_{ij}，V_{ij}　で以下の3条件を満足するものがあると仮定する。

1) U_{ij} , V_{ij} はすべて（0、1、-1）-行列である。即ち、成分が全て0か1か -1のいずれかである。

2) $U_{ij} \pm V_{ij}$ はすべて（1, -1）-行列である。

3) すべてのiに対して $e(U_{ii}) = 1$ であり、$i \neq j$ に対しては $e(U_{ij}) = 0$ である。

次に、$T_{ij} = U_{ij} \otimes \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + V_{ij} \otimes \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$ と $2m \times 2m$ 行列 T_{ij} を定義する。この時、条件2）より行列 T_{ij} は、（1、-1）-行列となる。即ち、T_{ij} の成分は1か -1である。さらに、$(2m+1) \times (2m+1)$ 行列 X_{ij} を次の様に構成する。

$$X_{ii} = \begin{bmatrix} 1 & -e_{2m} \\ -e_{2m}{}^t & T_{ii} \end{bmatrix}, \qquad X_{ij} = \begin{bmatrix} 1 & e_{2m} \\ e_{2m}{}^t & T_{ij} \end{bmatrix}$$

前者は $i = j$ に対してであり、後者は $i \neq j$ に対して定義する。T_{ij} と同様に X_{ij} も又（1、-1）-行列である。16個の $(2m+1) \times (2m+1)$ 行列が出来たので、最後に

$$H = W(X_{ij})$$

と置く。

Hは $4(2m+1) \times 4(2m+1)$ 正方行列で、その成分は1か -1である。主定理は U_{ij} と V_{ij} に対する簡単な

仮定のもとに、Hがアダマール行列となることを示す。

まず、$U = W(U_{ij})$, $V = W(V_{ij})$と置く。

<u>主定理</u>. もし $UU^t = (2m+1)I_{4m} - 2I_4 \otimes J_m$ と $VV^t = (2m+1)I_{4m}$ が両方成立つなら、$H = W(X_{ij})$ はアダマール行列となる。さらに、U と V とが両方とも Williamson型なら、Hも又 Williamson型となる。

証明の概略. $H = W(X_{ij})$の各行各列の内、各 X_{ij} の第1行と第1列とを前に取り出して、次の様に変形できる。

$$\begin{bmatrix} W(1,1,1,1) & W(-e,e,e,e) \\ W(-e^t,e^t,e^t,e^t) & W(T_{ij}) \end{bmatrix}$$

行の交換と列の交換だけなので、これがアダマール行列であることを示せば良い。この行列の上の部分列

$$W(1,1,1,1) \quad W(-e,e,e,e)$$

は実際には4列からなっている。 又、簡単な計算によって、$W(T_{ij})$ が Williamson型であれば、$W(X_{ij})$ も又 Williamson型となることが分る。条件3)より、$e(T_{ii}) = 2$, また $i \neq j$ に対しては、$e(T_{ij}) = 0$ が成立つので、上の4列と

下の5列以降とはお互に直交している。又、上の4列も互に直交しているので、後は、

$$W(T_{ij})W(T_{ij})^t = (8m+4)I_{8m} - 4I_4 \otimes J_{2m}$$

を示せば良い。これは、主定理の仮定から単純な計算によってでてくる。

定理1の証明を例にとって示そう。

奇素数巾qで、$q \equiv 1$（法4）と成るものに対してq＋1次（即ち2m＋2×2m＋2の）C－行列

$$C = \begin{bmatrix} 0 & 1 & e & e \\ 1 & 0 & e & -e \\ e^t & e^t & -C_1 & C_2 \\ e^t & -e^t & C_3 & C_4 \end{bmatrix}$$

が存在する。C_i は4つともm×m行列である。　又、仮定より、2m次のアダマール行列

$$K = \begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix} \quad (K_i \text{ はm×m行列})$$

が与えられているので、

$$U = \begin{bmatrix} C_1 & C_2 & 0 & 0 \\ -C_3 & C_4 & 0 & 0 \\ 0 & 0 & C_1 & C_2 \\ 0 & 0 & -C_3 & C_4 \end{bmatrix}$$

$$V = \begin{bmatrix} I & O & K_1 & K_2 \\ O & I & K_3 & -K_4 \\ -K_1^t & -K_3^t & I & O \\ -K_2^t & K_4^t & O & I \end{bmatrix}$$

と置くと主定理の仮定を満たしている。

定理４の証明は仮定よりＶがWilliamson型となり、又、体の性質からＵも又、Williamson型と取れるので、結局Ｈも Williamson型となる。他の定理や系の証明も同様にして得られる。

知られているアダマール行列の表。

この表に載っていない２０００まで奇素数ｎに対しては、４ｎ次のアダマール行列がみつかっている。又、表の中の　ｎ（ｓ）　は　$2^s n$ 次のアダマール行列が存在している事を意味する。

103 (3),	163 (3),	167 (3),	179 (3),	191 (3),
213 (3),	223 (3),	239 (4),	251 (3),	283 (3),
311 (3),	347 (3),	359 (4),	419 (4),	443 (3),
463 (3),	479 (12),	487 (3),	491 (4),	523 (3),
537 (4),	571 (3),	573 (3),	599 (4),	631 (3),
643 (3),	647 (3),	653 (3),	659 (17),	669 (3),
719 (4),	739 (4),	749 (4),	751 (3),	781 (3),
787 (3),	789 (3),	823 (3),	839 (8),	853 (3),

859 (3), 883 (3), 907 (3), 917 (3), 919 (3),
933 (4), 947 (4), 955 (3), 971 (4), 991 (3),
1019 (4), 1031 (4), 1039 (3), 1051 (3), 1063 (3),
1087 (4), 1103 (3), 1115 (4), 1123 (3), 1169 (4),
1177 (4), 1187 (3), 1223 (8), 1255 (3), 1257 (5),
1259 (4), 1283 (3), 1291 (3), 1303 (3), 1315 (3),
1319 (12), 1327 (4), 1349 (3), 1367 (3), 1423 (3),
1427 (3), 1439 (12), 1441 (3), 1447 (4), 1451 (4),
1471 (3), 1473 (3), 1483 (3), 1487 (3), 1491 (3),
1499 (16), 1507 (3), 1509 (3), 1543 (3), 1559 (4),
1567 (4), 1571 (4), 1579 (5), 1583 (3), 1589 (3),
1619 (4), 1633 (3), 1663 (4), 1667 (3), 1689 (3),
1699 (3), 1703 (3), 1713 (4), 1719 (3), 1723 (3),
1747 (3), 1783 (4), 1787 (3), 1793 (4), 1795 (5),
1823 (3), 1831 (3), 1841 (3), 1847 (3), 1871 (3),
1879 (3), 1883 (4), 1893 (4), 1907 (3), 1915 (3),
1929 (4), 1949 (4), 1969 (4), 1979 (4), 1981 (4),
1987 (4),

参考文献

1. A.V.Geramita and J.Seberry, "Orthogonal Designs," Lecture Notes in Pure and Applied Math., 45, Marcel Dekker, New York-Basel, (1979).

2. M.Yamada, Some new series of Hadamard matrices, J. Australian Math. Soc., (to appear).